UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/710,380	11/10/2000	Arthur R. Hair	HAIR-22	5438

7590 02/09/2006

Ansel M Schwartz
One Sterling Plaza
201 N Craig Street
Suite 304
Pittsburgh, PA 15213

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 02/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/710,380	HAIR ET AL.	
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/08/2005 has been entered. Claims 1-6 are pending.

Response to Arguments

2. Applicant's arguments filed 12/08/2005 have been fully considered but they are not persuasive. Applicant argues that the two context of Roger and Matyas are totally distinct and talking the teachings of Matyas and trying to apply it to Roger will totally change the intent and purpose of Roger and therefore claim 1 is patentable over Roger in view of Matyas. Applicant argues that Examiner is using the hindsight from applicant's own claim to combine the reference to arrive at applicants' claimed invention. Applicant further argues that the same arguments apply to the combination of Olson in view of Matyas. Examiner respectfully disagrees.

3. Examiner would point out that In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In*

re McLaughlin, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). Examiner would further point out Roger teaches a trusted and decentralized peer-to-peer network, wherein each server hosts data from other servers and data moves from one server to another every so often partly based on each server's trust of the others [see for example page 55, paragraph 3]. Roger further teaches data retrieval where a node retrieves data from one of the servnet nodes by gaining access to the public key that was used to sign the data [see for example page 60, paragraph 4]. Therefore, based on the trust between different servers, published data is transmitted between multiple servers, which implies control of the data is passed on to other trusted servers. Furthermore peer-to-peer key distribution method is well known in the art. Matyas teaches a peer-to-peer key distribution method including, a host computer sending a public key to a first of the 2 computing devices [see, for example figure page 185, figure 7, C sends key to A] and the first computing device sending the public key to a second of the 2 computer devices [see for example, page 185, figure 7, A sends key to B] through the communication means to establish the decentralized trusted network [pages 185-186 Key-distribution environments, *peer to peer and key distribution center*]. Examiner asserts that the combination of Rogers in view of Matyas and Olson in view of Matyas teach the claim limitations and therefore the rejection is respectfully maintained.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roger R. Dingledine, "The Free Haven Project: Design and Deployment of Anonymous Secure Data Haven", May 22, 2000 (hereinafter Roger) in view of Matyas et al "A key-management scheme based on control vectors", IBM Systems Journal, Vol. 30, No 2, 1991 (hereinafter Matyas).

6. As per claim 1, Roger teaches a system to establish a trusted and decentralized peer-to-peer network comprising:

communication means [page 55, paragraph 2];

n user computing devices connected to the communication means, where n is greater than or equal to 1 and is an integer [page 55, paragraphs 2 & 3]; and

a host computing device connected to the communication means having a mechanism to establish a decentralized trusted communication network with at least 2 of the n users computing devices through which digital signals are shared securely between the host computing device the 2 users computing devices of the trusted communication network [page 55, paragraphs 3 & 4 and page 7]. Roger does not explicitly teach sending a public key to a first of the 2 user computer devices and the first user computing device sending a public key to a second of the 2 user computer devices through the communication means to establish the decentralized trusted network. However, peer-to-peer key distribution method is well known in the art. For example Matyas teaches a peer-to-peer key distribution method including, a host computer sending a public key to a first of the 2 computing devices [see, for example figure page 185, figure 7, C sends key to A] and the first computing device sending the public key to a second of the 2 computer devices [see for example, page 185, figure 7, A sends key to B] through the communication means to establish the decentralized trusted network [pages 185-

186 Key-distribution environments, *peer to peer and key distribution center*]. One of ordinary skill in the art would have been able to modify the teachings of Matyas within Roger in order to distribute encryption keys in peer-to-peer environment. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the key distribution method taught by Matyas within the secure decentralized system of Roger to achieve the advantage of providing key distribution in peer-to-peer environment between peer computing devices.

7. As per claim 2, Roger teaches, a method of establishing a trusted and decentralized peer-to-peer network comprising the steps of:

sending a public key from a host computing device to communication means connected to the host computing device [page 72, paragraph 1];

receiving the public key at a first user computing device connected to the communication means [page 72, paragraph 1 and 2];

receiving the public key at a second user computing device to establish a decentralized trust communication network between the host computing device, the first and the second computing device through which digital signals are shared securely between the host computing device, the first user computing and second user computing device, sending digital signals directly from the first user computing device securely to the second user computing device [page 55, paragraph 4 and page 60, paragraph 4].

Roger does not explicitly teach sending a public key to a first of the 2 user computer devices and the first user computing device sending a public key to a second of the 2 user computer devices through the communication means to establish the decentralized trusted network. However, peer-to-peer key distribution method is well known in the art. For example

Matyas teaches a peer-to-peer key distribution method including, a host computer sending a public key to a first of the 2 computing devices [see, for example figure page 185, figure 7, C sends key to A] and the first computing device sending the public key to a second of the 2 computer devices [see for example, page 185, figure 7, A sends key to B] through the communication means to establish the decentralized trusted network [pages 185-186 Key-distribution environments, *peer to peer and key distribution center*]. One of ordinary skill in the art would have been able to modify the teachings of Matyas within Roger in order to distribute encryption keys in peer-to-peer environment. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the key distribution method taught by Matyas within the secure decentralized system of Roger to achieve the advantage of providing key distribution in peer-to-peer environment between peer computing devices.

8. As per claim 3, the combination of Roger and Matyas teaches the method as applied above. Furthermore, Matyas teaches creating encryption and decryption keys [page 185-186 Key-distribution environments, *peer to peer and key distribution center*].

9. As per claims 4 and 5, the combination of Roger and Matyas teaches the method as applied above. Furthermore, Roger teaches the method including creating a searchable ciphertext containing identifiable network information on each computing device which is shared with every other computing device [page 60, paragraphs 3-5].

10. As per claim 6, the combination of Roger and Matyas teaches the method as applied above. Furthermore, Roger teaches the method including the step of finding by a member of the

trusted peer-to-peer network other members of the trusted peer-to-peer network [page 60, paragraphs 3-5].

11. Claims 1-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olson et al. (U.S. Patent No. 6,311,209 B1) (hereinafter Olson) in view of Matyas et al "A key-management scheme based on control vectors", IBM Systems Journal, Vol. 30, No 2, 1991 (hereinafter Matyas).

12. As per claim 1, Olson teaches a system to establish a trusted and decentralized peer-to-peer network comprising:

communication means [figure 1, unit 12];

n user computing devices connected to the communication means, where n is greater than or equal to 1 and is an integer [figure 1 units 14, 16 and 18]; and

a host computing device connected to the communication means having a mechanism to establish a decentralized trusted communication network with at least 2 of the n users computing devices through which digital signals are shared (i.e. each client maintaining a copy of data throughout an application session, and each time client changes application data the change is communicated to all other clients, e.g. client A, B and C of Fig 1 maintaining a copy of data at elements 20, 22 and 24) [column 6, lines 29-41] securely between the host computing device and the 2 users computing devices of the trusted communication network [column 3, lines 30-41, column 6, lines 47-53 and column 2, lines 22-27].

Olson does not explicitly teach sending a public key to a first of the 2 user computer devices and the first user computing device sending a public key to a second of the 2 user computer devices through the communication means to establish the decentralized trusted

network. However, peer-to-peer key distribution method is well known in the art. For example Matyas teaches a peer-to-peer key distribution method including, a host computer sending a public key to a first of the 2 computing devices [see, for example figure page 185, figure 7, C sends key to A] and the first computing device sending the public key to a second of the 2 computer devices [see for example, page 185, figure 7, A sends key to B] through the communication means to establish the decentralized trusted network [pages 185-186 Key-distribution environments, *peer to peer and key distribution center*]. One of ordinary skill in the art would have been able to modify the teachings of Matyas within the system of Olson in order to distribute encryption keys in peer-to-peer environment. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the key distribution method taught by Matyas within the secure decentralized system of Olson to achieve the advantage of providing key distribution in peer-to-peer environment between peer computing devices.

13. As per claim 2, Olson teaches a method of establishing a trusted and decentralized peer-to-peer network comprising the steps of:

sending a public key from a host computing device to communication means connected to the host computing device [column 3, lines 35-40];

establishing a decentralized trust communication network between the host computing device, a new client and existing clients by forwarding the public key to the new and existing clients [column 3, lines 35–40 and column 8, lines 12-21] through which digital signals are shared (i.e. each client maintaining a copy of data throughout an application session, and each time client changes application data the change is communicated to all other clients e.g. client A, B and C of Fig 1 maintaining a copy of data at elements 20, 22 and 24) [column 6, lines 29-

41] securely between the host computing device and the client computing devices, and sending digital signals directly from the user computing device securely to the second computing device [column 3, lines 30-42, column 6, lines 47-53 and column 2, lines 22-27].

Olson does not explicitly teach sending a public key to a first of the 2 user computer devices and the first user computing device sending a public key to a second of the 2 user computer devices through the communication means to establish the decentralized trusted network. However, peer-to-peer key distribution method is well known in the art. For example Matyas teaches a peer-to-peer key distribution method including, a host computer sending a public key to a first of the 2 computing devices [see, for example figure page 185, figure 7, C sends key to A] and the first computing device sending the public key to a second of the 2 computer devices [see for example, page 185, figure 7, A sends key to B] through the communication means to establish the decentralized trusted network [pages 185-186 Key-distribution environments, *peer to peer and key distribution center*]. One of ordinary skill in the art would have been able to modify the teachings of Matyas within the method of Olson in order to distribute encryption keys in peer-to-peer environment. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the key distribution method taught by Matyas within the secure decentralized system of Olson to achieve the advantage of providing key distribution in peer-to-peer environment between peer computing devices.

14. As per claim 3, the combination of Olson and Matyas teaches the method as applied above. Furthermore, Matyas teaches creating encryption and decryption keys [page 185-186 Key-distribution environments, *peer to peer and key distribution center*].

Conclusion

15. All claims are drawn to the same invention claimed in the application prior to the entry of the submission under 37 CFR 1.114 and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered in the application prior to entry under 37 CFR 1.114. Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action after the filing of a request for continued examination and the submission under 37 CFR 1.114. See MPEP § 706.07(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

February 3, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100